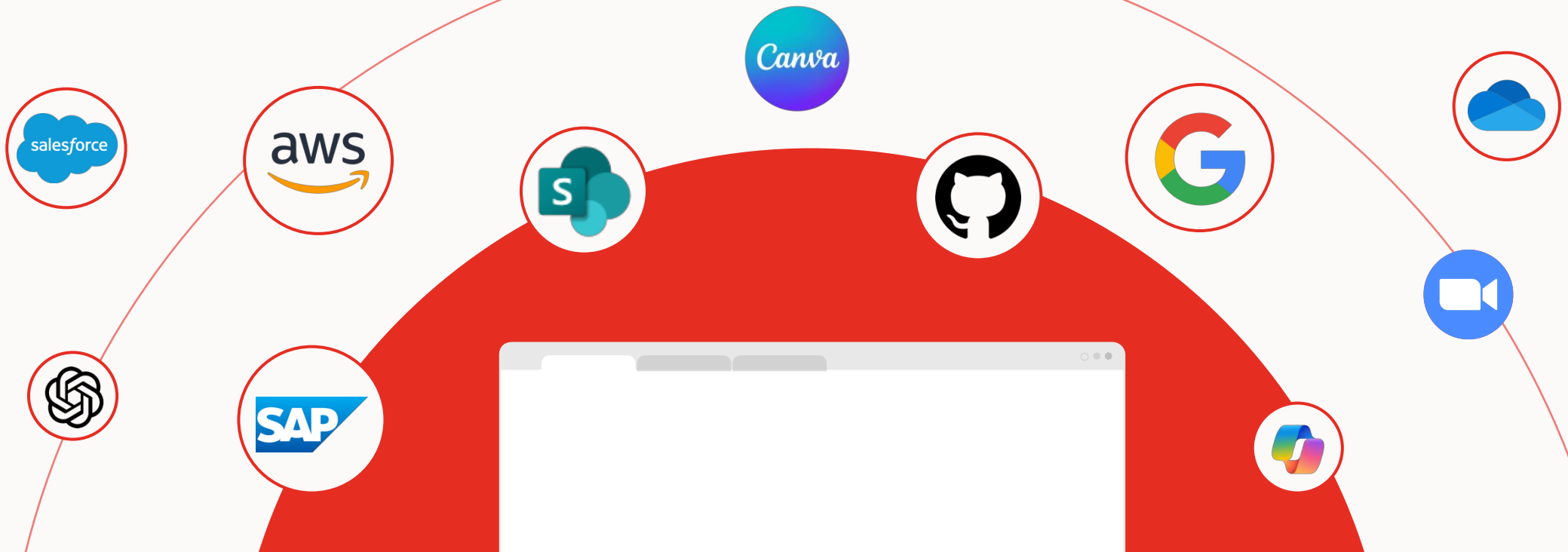
ERMES

BROWSER SECURITY

ERMES
BROWSER SECURITY

Your business runs on the Browser.



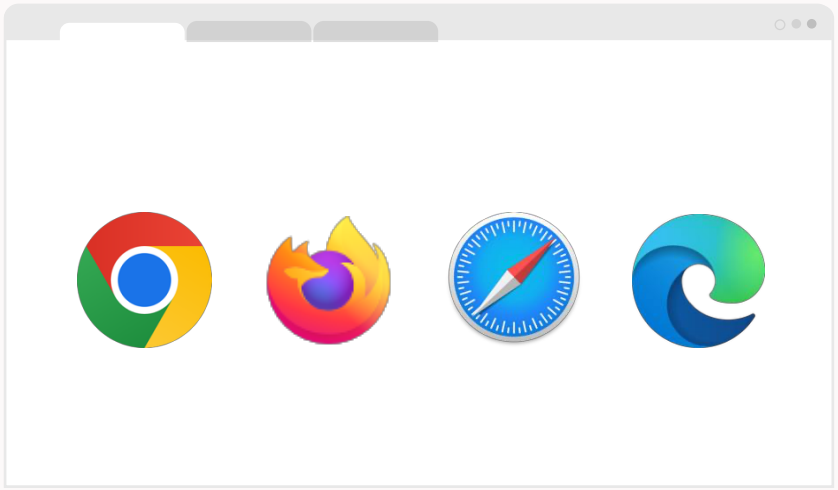
ERMES
BROWSER SECURITY

CASB

EDR

ZTNA

MDR



SIEM

ANTI-SPAM

DLP

FIREWALL

SOC

But no system

protects your Browser

ERMES
BROWSER SECURITY

+90% "of cyberattacks start from a web page"
Google Security Report
Google

70%+ "of malware is delivered via the browser"
Verizon DBRI
verizon

The browser has become **the weakest link** in Zero Trust architectures

Forrester, "Securing the Last Mile" FORRESTER

90% "of modern phishing now use simulated web pages, no longer just email-based"
APWG Phishing Trends Report 2024
APWG

300% "in attacks leveraging JavaScript, cloaking techniques, and browser based"
SANS Institute, ThreatLabZ
SANS

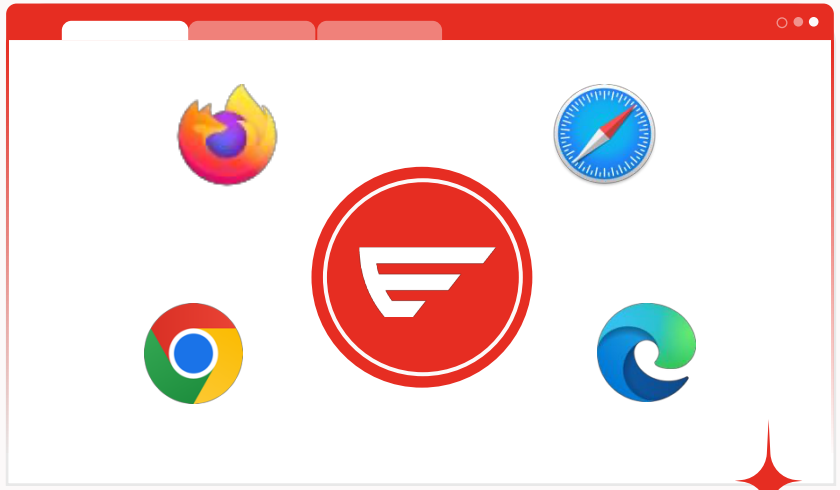
ERMES
BROWSER SECURITY

CASB

EDR

ZTNA

MDR



ANTI-SPAM

SIEM

DLP

FIREWALL

SOC

We make Browsers Enterprise.

ERMES
BROWSER SECURITY

Browser-Native Architecture

Built to protect what others can't.

With an extension for most used browser.
No isolation, more use cases.

We make your Browser Enterprise.

AI Proprietary Intelligence

NO VPN

NO SSL INSPECTION
FULL VISIBILITY

NO PROXY

- Zero infrastructures
- Easy to deploy
- Invisible for the user
- On device protection
- **TOP 10** Browser Security vendor

ERMES
BROWSER SECURITY

One extension,

Three Protection Layers

Many use cases

SESSION Protection

AI Based Protection

Contextual DLP

Launching in Q1 2026

– a new way to protect what matters

ERMES
BROWSER SECURITY

SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

Browser Extension Protection

Advanced Web Filtering

Browsing Risk Assessment

Enterprise control

over People Behavior

SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

Browser Extension Protection

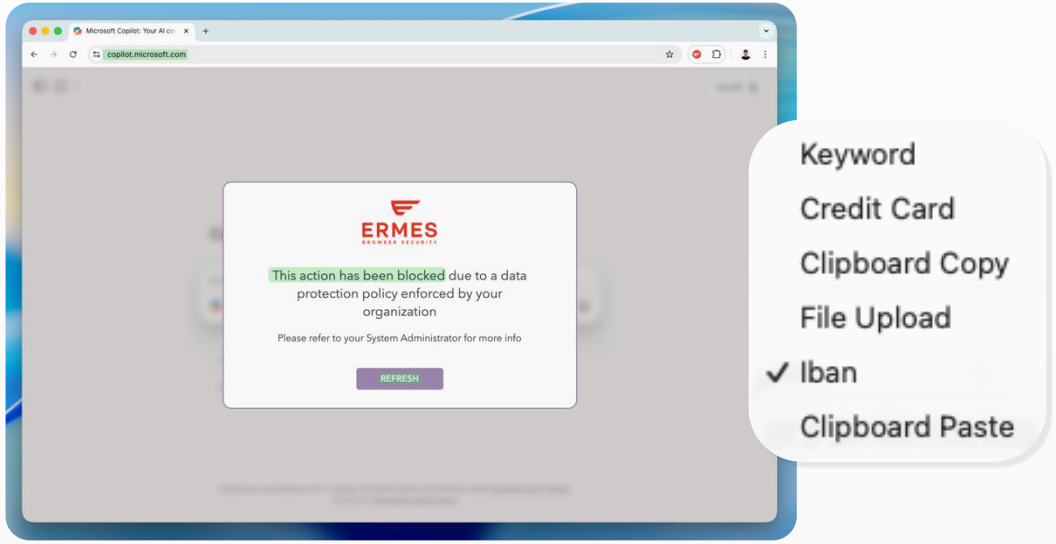
Advanced Web Filtering

Browsing Risk Assessment

Can you maintain **Full Visibility and Enforce Policies** on corporate data — without impacting daily work?

With Ermes, yes. You gain **complete oversight into everything happening on the web**—GenAI, personal email, messaging, file repositories, and more—while keeping employees productive.

We both **Block** and **Audit**



SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

Browser Extension Protection

Advanced Web Filtering

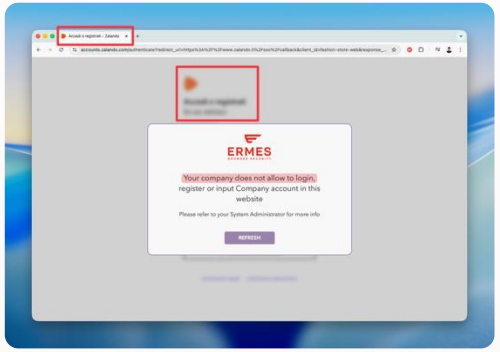
Browsing Risk Assessment

Gartner

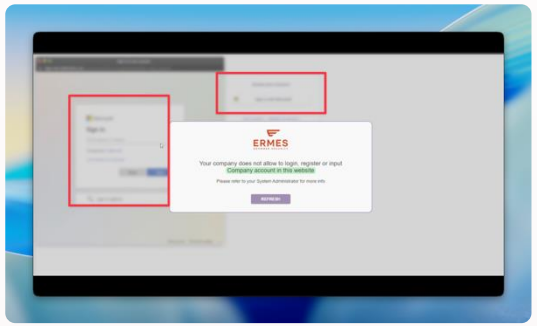
We **prevent leakage** of Business Credentials, and we show shadow IT

We prevent users to use their company email/usernames on **unsactioned web apps in real time**. We allows companies to audit business credential usage and discover unsanctioned apps accessed by users:

With BCP we act as the last mile of defense against phishing: even if an advanced attack reaches the user, this module physically prevents them from entering their email and losing credentials:



Simulation on zalando



Phishing simulation over MS365 Account with MFA exfiltration

Microsoft

SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

Browser Extension Protection

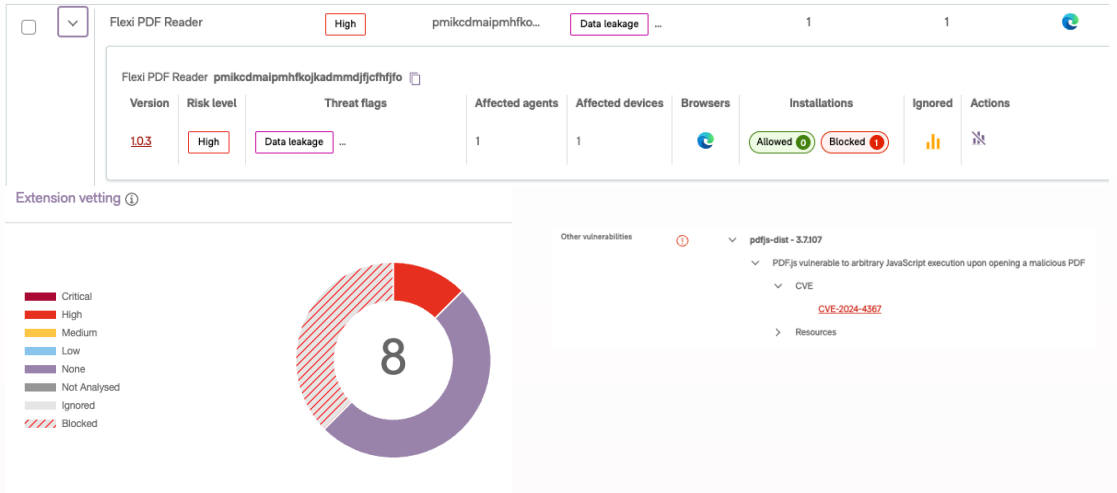
Advanced Web Filtering

Browsing Risk Assessment

Gartner

NIS2 Network & Information Systems Directive

Under the NIS2 directive, companies must manage vulnerabilities, security patches, cyber hygiene, and control over **all installed software**... are you sure you can control it all?



Detects and **make policies** about vulnerable, risky and malicious browser extensions installed by users

It controls:

- Malicious traits
- Execution patterns via code analysis
- Permissions requested
- Dependencies vulnerabilities
- Reputation and presence on official stores

Browser extensions represent the most dangerous software of the browser and a wide source of Shadow IT.

SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

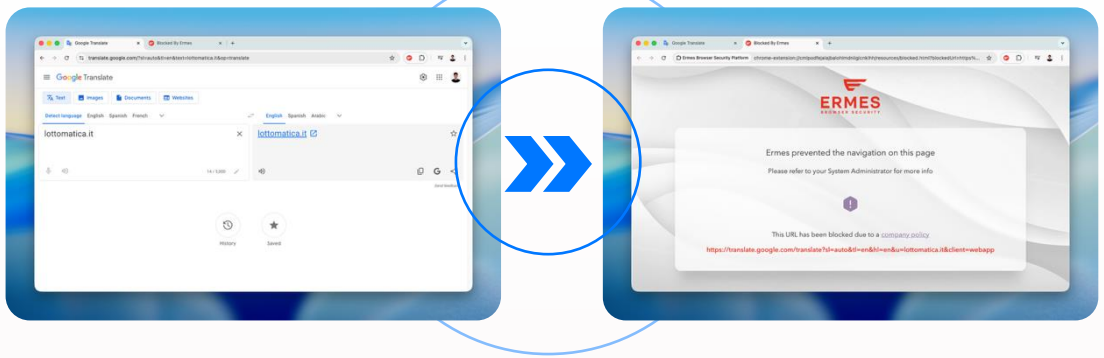
Browser Extension Protection

Advanced Web Filtering

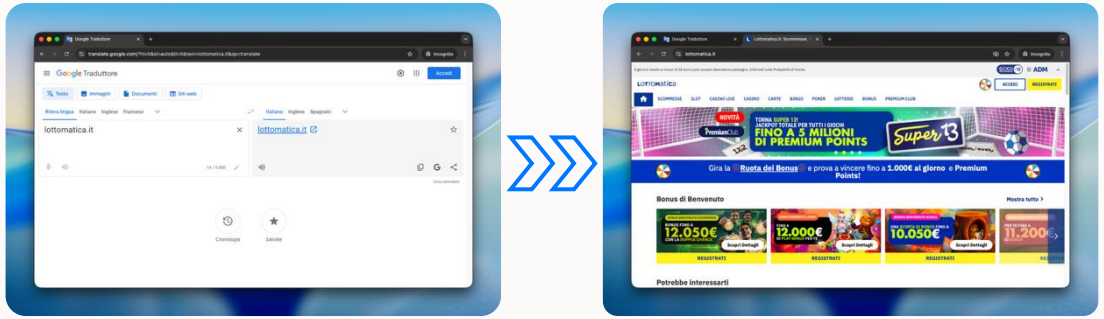
Browsing Risk Assessment

Allows to **block** or **authorize** access to websites based on their categorization with a proprietary AI-based engine.

With Ermes



Without Ermes



ERMES
BROWSER SECURITY

SESSION Protection

Use cases:

Web Data Loss Prevention

Business Credentials Protection

Browser Extension Protection

Advanced Web Filtering

Browsing Risk Assessment

Your always-on **governance cockpit** to monitor, measure, and reduce browser risk — aligned with NIST 2.0

CISOs and Security Managers can control risks caused by human factor and quantify effectiveness of their remediation strategies.
Native integration with SIEMs/SOARs or log export APIs

Microsoft Sentinel · splunk> · SGBOX · Radar · LOGPOINT

ERMES
BROWSER SECURITY

AI BASED Protection

Use cases:

Zero Day Phishing

Cybersquatting

Anti-tracking and Malvertising

NEW AI Real Time Protection

AI at the Edge,

Protection at the Speed of the Web

AI BASED Protection

Use cases:

Zero Day Phishing

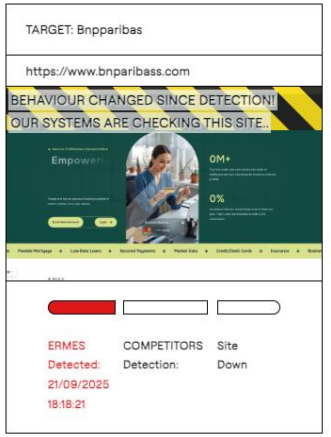
Cybersquatting

Anti-tracking and Malvertising

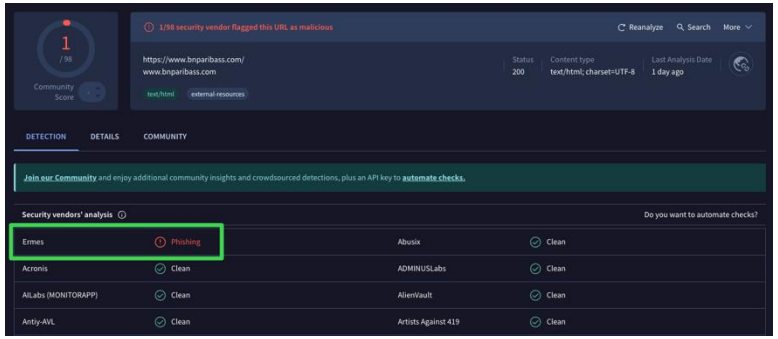
NEW AI Real Time Protection

“ What if a **malicious link slips** past your anti-phishing system and the user opens it in the browser?

By adding a **Browser Security layer**, you ensure protection with an extremely advanced AI-powered crawler



certified by VirusTotal



AI Web Crawler

A **new** leading edge, AI-based, behavioral proprietary **Anti-Phishing Engine**. Ermes **analyzes all new domains** registered on the internet, checking more than **300 attributes**.

See it: https://www.ermes.company/live

AI BASED Protection

Use cases:

Zero Day Phishing

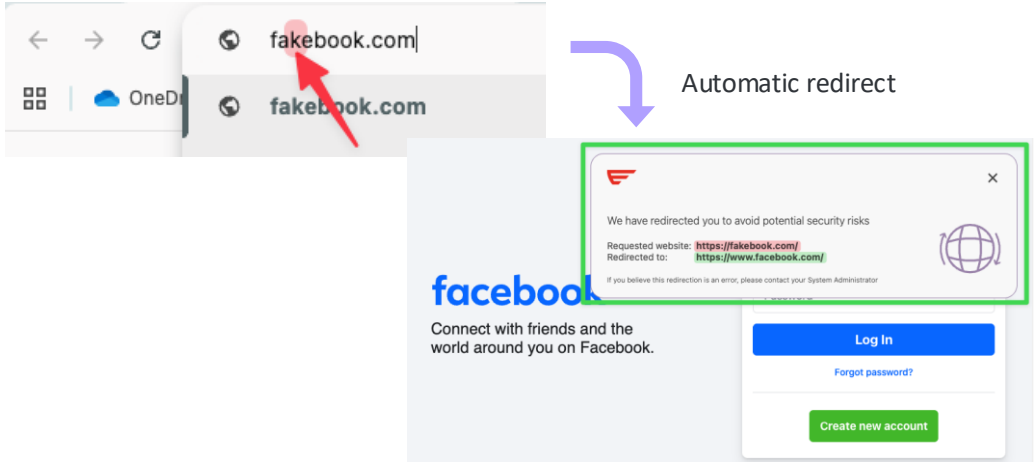
Cybersquatting

Anti-tracking and Malvertising

NEW AI Real Time Protection

"What happens when a user clicks on **a domain that looks just like the real one**?

They could fall into an attack — even while trying to access a **supplier, partner, or customer's site**



Machine Learning

Ermes uses a **proprietary combination** of **blocklisting** and **AI** to protect users navigation. **Real-time ML** analyzes attacks based on cybersquatting and behavioral errors.

By default protection includes top visited domains. It can be enhanced with personalized domains for enterprise customers

AI BASED Protection

Use cases:

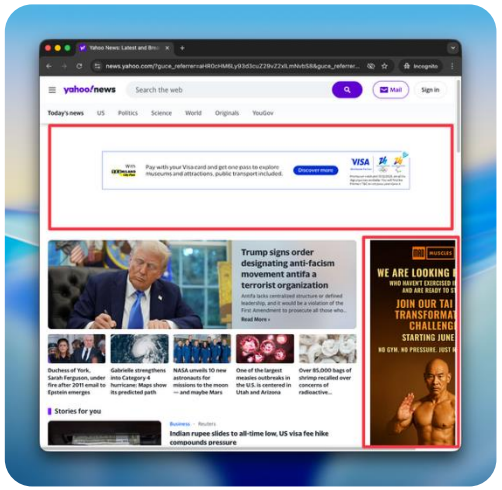
Zero Day Phishing

Cybersquatting

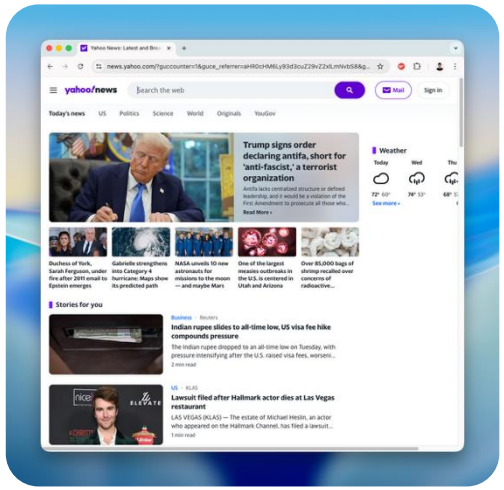
Anti-tracking and Malvertising

NEW AI Real Time Protection

Without Ermes



With Ermes



STOP Online ads

STOP Malvertising

STOP Web Trackers

STOP Cryptominers

STOP Noise on SIEMs and network systems

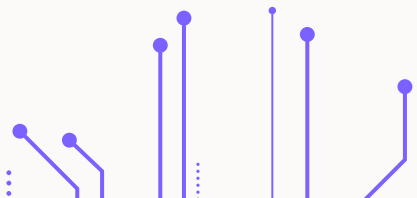
REDUCES Bandwidth usage & network workload

IMPROVES User navigation experience

ERMES
BROWSER SECURITY

NEW

AI Real Time Protection.



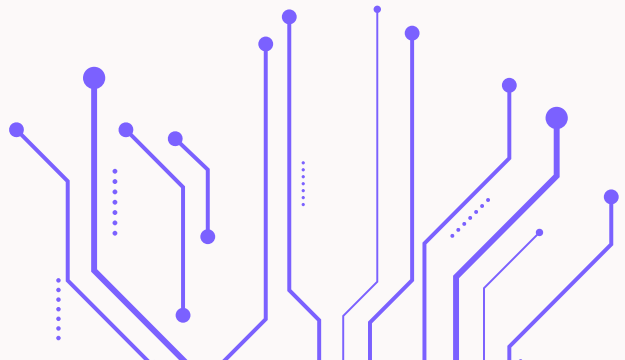
ERMES
BROWSER SECURITY

AI technologies leverage the cloud

to detect threats and instantly communicate them

to the browser extension

But now,
we do even more

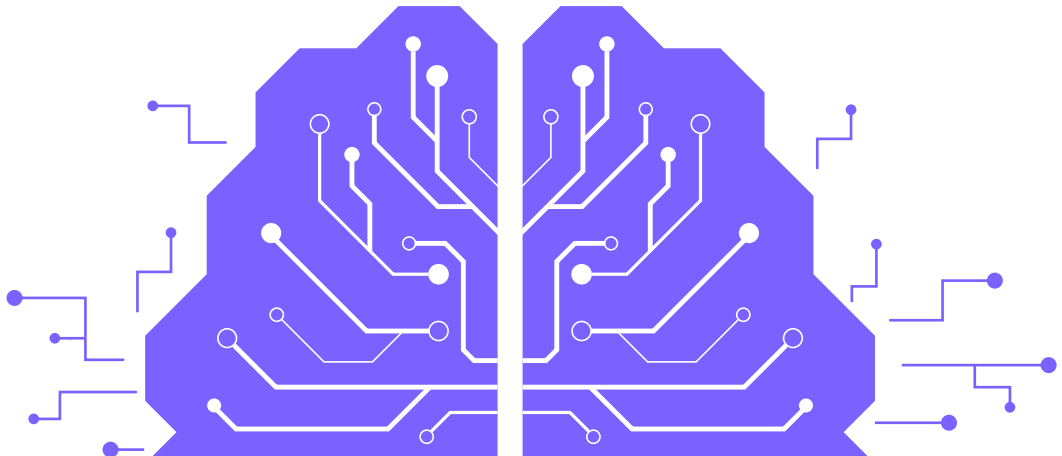


ERMES
BROWSER SECURITY

Now we have a

Neural Engine

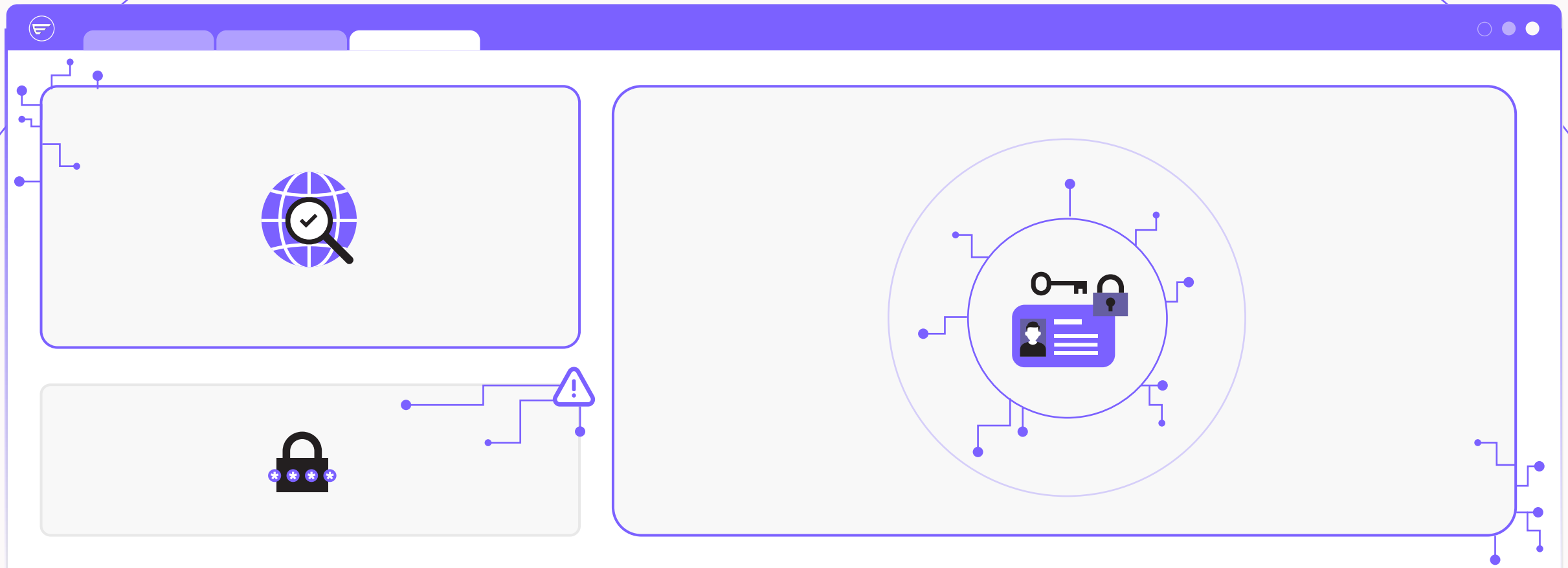
Inside the Browser Extension



ERMES
BROWSER SECURITY

Neural Engine

To discover Real Threats in Real Time



ERMES
BROWSER SECURITY

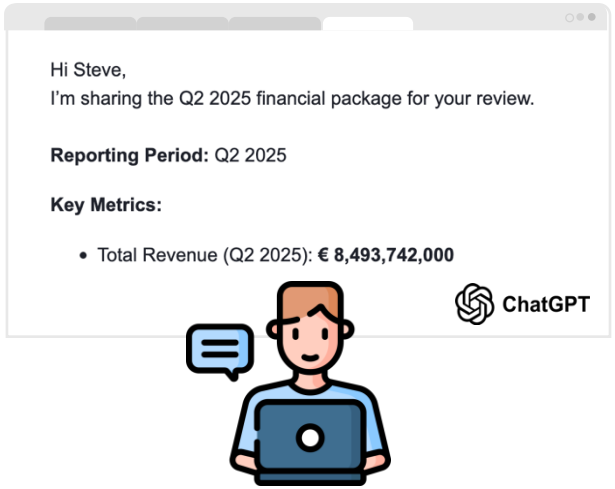
Launching Q1 2026

Contextual DLP

a new way to protect what matters

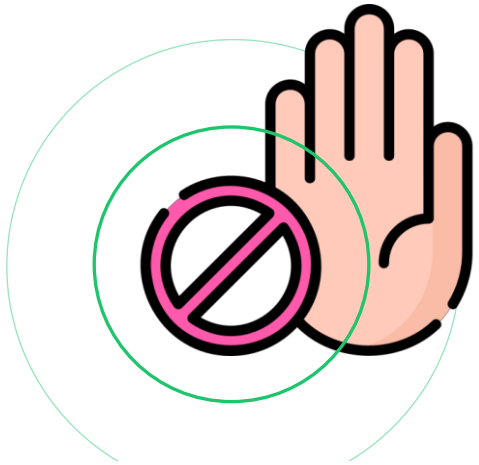
Contextual DLP - **Block**

User Action



An employee pastes the text of an email containing financial data into ChatGPT to speed up the analysis of results and send a comment to their manager.

Protect



The system detects sensitive content **and blocks the action**.

Security Awareness & Guidance

You are sharing corporate financial information with an unauthorized web application.

The data is sensitive and must not be shared.

And invite users to use Corporate tools for this kind of tasks.

OK

Use case of protection against data leakage thanks to **context-aware protection based on LLM**

Contextual DLP – **Data Masking**

User Action

John Smith
1234 Elm St, Springfield, IL 62701
jane.doe@example.com
(555) 123-4567

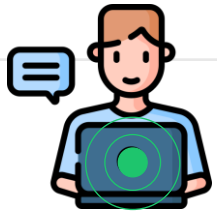
Gemini

A user pastes a client's personal information into an authorized web service.

Protect

[NAME]
[PHYSICAL ADDRESS]
[EMAIL ADDRESS]
[PHONE NUMBER]

Gemini



The system automatically anonymizes sensitive data contextually.

Security Awareness & Guidance

You are sharing personal information.

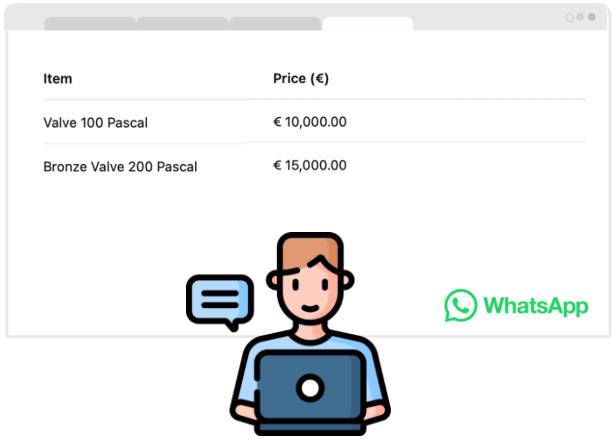
The data has been masked in order to be shared.

OK

Use case of sensitive data identification and **automatic data masking**

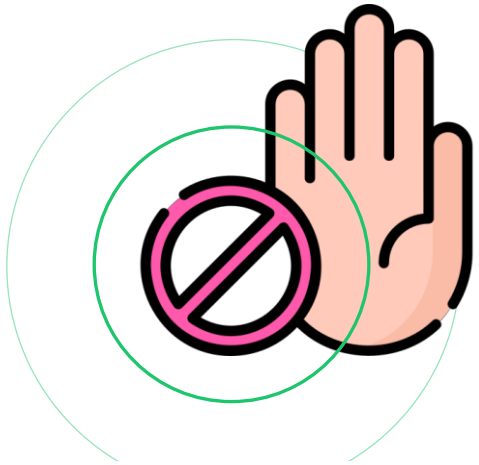
Contextual DLP - **Bypass**

User Action



An employee downloads the product price list from SharePoint and shares it via WhatsApp Web, which is a corporate tool, but the employee is not allowed to share this type of data externally.

Protect



The system detects sensitive content **and blocks the action**.

Security Awareness & Guidance

A warning appears for the user: this tool can be used, but this type of data cannot be shared externally.

OK

Use case of protection against data leakage thanks to **context-aware protection based on LLM**

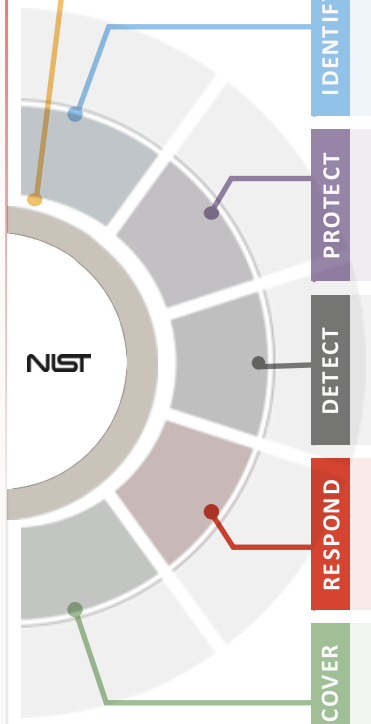
Mobile Guardian

Use cases:

- Malvertising & Tracking Protection
- Advanced Web Filtering
- Web Data Loss Prevention
- Zero Day Phishing
- Cybersquatting
- Real Time Protection
- Business Credential Protection
- Browsing Risk Assessment

ERMES BROWSER SECURITY & NIST 2.0

NIST CYBERSECURITY FRAMEWORK



		AI Based Protection	Session Protection
GOVERN	*Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy*	Logs can be used to define a Browser Security hardening strategy and monitor it	
IDENTIFY	*Help determine the current cybersecurity risk to the organization*		Full visibility on shadow SAAS
PROTECT	*Use safeguards to prevent or reduce cybersecurity risk*	AI protection against emerging attacks	Policy enforcement to reduce shadow SAAS.
DETECT	*Find and analyze possible cybersecurity attacks and compromises*	Logs can be used to detect attacks	
RESPOND	*Take action regarding a detected cybersecurity incident*	Logs can be used to investigate attacks	
RECOVER	*Restore assets and operations that were impacted by a cybersecurity incident*	Not in Ermes Browser Security Platform Scope.	

Ermes is a **CyberSecurity software vendor certified** as made in Europe and represents the greatest Italian start-up in cybersecurity field with more than 8M$ of investments

Gartner · FORRESTER · CYBERSECURITY MADE IN EUROPE · CERTIFIED ISO 27001 ISO 27017 ISO 27018 · Great Place To Work. Certified ITALIA · Best Workplaces for Millennials Great Place To Work. ITALIA 2022

2018
founded as a spin-off by Politecnico di Torino

10 +
Proprietary AI Methodologies

+100.000
devices protected

European
product and company

Top World Solution
certified by Gartner

Marketplace available: aws · Microsoft · Google

Business Case Analysis

IBSA (Institut Biochimique SA) is a Swiss multinational pharmaceutical Company, founded in 1945 in Lugano. Today, its products are present in over 90 Countries on 5 continents, through the Company's 20 subsidiaries located in Europe, China, and the United States. The company has a turnover of CHF 1.089 billion and employs over 2,500 people between headquarters, subsidiaries and production sites. IBSA holds a vast portfolio of products, covering 10 therapeutic areas: reproductive medicine, endocrinology, pain and inflammation, osteoarticular, aesthetic medicine, dermatology, uro-gynaecology, cardiometabolic, respiratory, consumer health. It is also one of the largest operators worldwide in the area of reproductive medicine, and one of the world's leaders in hyaluronic acid-based products. IBSA has based its philosophy on four pillars: Person, Innovation, Quality and Responsibility.

IBSA source

Davide Meloni,
IBSA CISO

"It's not always possible to solve everything internally. Collaboration with dynamic, specialized companies allows us to accelerate our responses and create tailor-made solutions".

Chosen by Market Leaders and Innovators

MAIRE, TIM, Carrefour, KPMG, IBSA, FAAC, SOLGROUP a breath of life, Romagna Acque Società delle Fonti, TIGROS
cefla, DUMAREY, BonelliErede, BALOCCO, GRUPPO CREMONINI, CHIOMENTI, Fratelli Beretta 1812, LA7, ALFAGOMMA, Aeroporto di Bologna, ABS
FHP Group, AirDolomiti, Cuki, facile.it, Gruppo Montenegro, urmet, sorgenia, IVECO DEFENCE VEHICLES, BANOR, Marchesi ANTINORI, DISARONNO

Fueling Europe's Future:

Empowering Innovation through
University–Industry Collaboration

6.2mln € 2025-28

in R&D

Politecnico di Torino

ERMES BROWSER SECURITY

AI4CTI – Advancing Cybersecurity with AI:

A Strategic Research Partnership

AI4CTI – Artificial Intelligence for Cyber Threat Intelligence is a cutting-edge research project born from the collaboration between Politecnico di Torino and Ermes Cyber Security. Funded by the FISA program of the Italian Ministry of University and Research, the initiative exemplifies the power of synergy between academic excellence and real-world cybersecurity innovation.

The project aims to develop intelligent systems capable of detecting and preventing cyber threats in real time—leveraging AI to counter phishing, scareware, and social engineering attacks. By combining scientific research and Ermes' hands-on industry expertise, AI4CTI will deliver scalable, practical solutions to protect users directly on their devices and contribute to the broader cybersecurity ecosystem through open data sharing.

This partnership marks a key milestone in translating fundamental research into impactful, enterprise-grade technology.

MUR

Demo

Live demo with tailored use cases

Pilot

4-6 weeks, guided and supported by Ermes' CS Team.

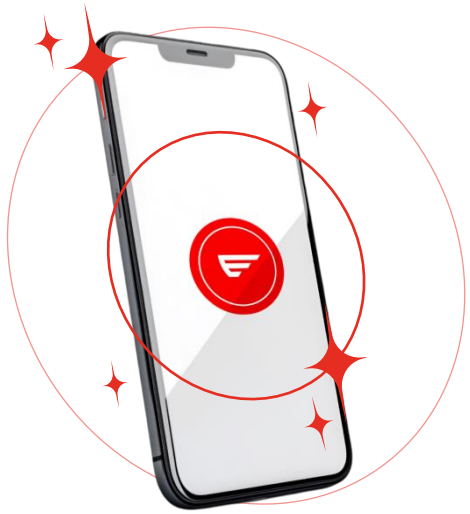
Browser Assessment Report

Live Presentation with key findings and next steps

Full Platform
Browser Security

N° PC Devices
3 Security Layers

From Q1 2026



N° Mobile Devices

with Managed Services

ERMES

BROWSER SECURITY